Wi-Fi and WiMAX: Protocols of Security

Judy M. Hartley

December 2007

Intel Corporation
## Contents

Abstract ................................................................................................................................ 3  
Introduction .......................................................................................................................... 3  
Wi-Fi Security Protocols .................................................................................................... 3  
WiMAX Security Protocols ............................................................................................... 4  
Security Attacks .................................................................................................................. 5  
Conclusion ........................................................................................................................... 6  
References ........................................................................................................................... 6  
About the Author ................................................................................................................. 7  

### Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Five Layer TCP/IP Model with Data Link Sub-Layers Shown</td>
<td>3</td>
</tr>
</tbody>
</table>
Abstract

With the growth of devices with WiMAX capabilities, it is time to take a close look at the security protocols found in WiMAX and compare them to those of Wi-Fi*. This article examines the WiMAX protocols and other security devices in some detail to determine the relative security of applications running over a WiMAX network. While the Wi-Fi protocols are fairly well documented, they will be described for the sake of completeness. Security attacks directed at both Wi-Fi and WiMAX are also discussed.

Introduction

Humans are creatures of habit on one hand and great believers in challenge and change on the other. Since the release of Wi-Fi Legacy (the original 802.11 standard) in 1997 [1], the majority of wireless internet communication has used some version of 802.11. Now a new standard, 802.16 or WiMAX, promises a new communication protocol with greater benefits. Unlike Wi-Fi’s unlicensed frequency bands, WiMAX devices work in a licensed frequency band and are capable of a greater range than Wi-Fi devices. Mobile platforms with WiMAX capabilities will soon be on the market. However, how secure is WiMAX? What security measures are in place for both of these wireless options?

For communication over the internet and between network devices, a suite of protocols is used to identify and route each packet of data that is sent and received. This suite uses the Transmission Control Protocol and Internet Protocol (TCP/IP). The suite provides protocols to handle five conceptual layers in the network implementation shown in Figure 1. As packets traverse the stack from bottom to top, they move from the network cable to the user. Both the Wi-Fi and WiMAX protocols are defined to implement layer 2 and layer 1 of the stack.

Figure 1. Five Layer TCP/IP Model with Data Link Sub-Layers Shown

| Layer 5 | Application |
| Layer 4 | Transport |
| Layer 3 | Network |
| Layer 2 | Data Link |
| Layer 1 | Physical |

| Logical Link Control |
| Media Access Control |

Wi-Fi Security Protocols

To form a foundation for the later discussion of WiMAX security, let’s review the Wi-Fi protocols. Wired Equivalency Privacy (WEP) was the first encryption method used for Wi-Fi. It uses the RC4 cipher for encryption and 128- or 256-bit keys are standard today. WEP was designed to provide roughly the equivalent of security provided by a wired connection. However, it was soon discovered that the encryption keys were not strong enough for today’s computing power. This protocol is still supported by many
devices today and has, often in the past, been the default choice during device setup. This protocol is still being used in many home networks.

In 2002, before the 802.11i standard was fully ratified, a new protocol was introduced. The Wi-Fi Protected Access (WPA) method implements stronger encryption algorithms and provides two usage levels. WPA-Personal is used in situations where there is no server for authentication. A “pre-shared key” (PSK) is created to authorize contact. This PSK is a phrase, 8 to 63 characters long, or a hexadecimal string up to 64 characters long, which is manually shared between access point and client. When an authentication server is available, WPA utilizes the 802.1X protocol to communicate with the server and dynamically assigns a different key for each attached device. A RADIUS server can be used to handle verification of those requesting access and enforcing policies for access. WPA provides greater security by changing the key often. Therefore, if a key is discovered by an outside entity, that key provides only a limited window of access to the network. To do this, WPA uses the Temporal Key Integrity Protocol (TKIP) to resets the 128-bit keys periodically. Optionally, the protocol provides support for AES-CCMP, a very strong security protocol that handles four security aspects (authentication, confidentiality, replay protection, and integrity).

WPA2 implements the required elements of the final ratification of the 802.11i specification that occurred in June of 2004. The primary difference between WPA and WPA2 is that the support of AES-CCMP protocol, optional in WPA, is now required in WPA2. Interestingly enough, WPA2 is not backward compatible, meaning that clients and access points must be reconfigured in order to switch between the two versions.

The final security device is the use of smart cards and USB tokens. Most of these devices carry strong forms of encryption that combine two or more types of authentication, such as biometrics and a password. Although this form of security is considered by some to be the strongest and safest, a drawback might be that it can be quite expensive. The higher cost would be due to the need for purchasing the physical devices for each employee and member of the team as well as supporting the authentication methods that are selected.

**WiMAX Security Protocols**

WiMAX was designed as a solution for the “last mile” of a Wireless Metropolitan Area Network (WMAN) that would bring internet access to an entire metropolitan area. There are two basic types of WiMAX, Fixed WiMAX and Mobile WiMAX. Fixed WiMAX is based on the 802.16-2004 standard and does not handle a base station transfer to another base station. For this reason, mobility is not supported. Implementations called Mobile WiMAX is based on the 802.16e-2005 amendment to the standard do support base-to-base transfer. From the start, WiMAX was designed with security in mind. At the lower-edge of the Media Access Control sub-layer of TCP/IP, a privacy sub-layer was defined in the official 802.16e-2005 specification to handle encryption of packets and key management. To handle authentication, the specification relies on the already existing Extensible Authentication Protocol (EAP) [2].

**The Privacy Layer**

There are two schemes for data encryption, which are supported in the 802.16 standard, the Advanced Encryption Standard (AES) and Triple Data Encryption Standard (3DES). Both of these schemes are block ciphers, which are security algorithms which operate on one chunk (or block) of data at a time vs. stream ciphers which can act on a single byte. AES handles a 128-bit block of data at a time, and has been shown to be very fast in both software and hardware implementations. Both because of its speed
and because of its ease to implement, AES has become the algorithm of choice for WiMAX. During the authentication process, a 128- or 256-bit key is created and that is used in conjunction with the cipher. Additionally, it is recreated at intervals for optimal security [3].

The 802.16e-2005 amendment specifies Privacy and Key Management Protocol Version 2 as the key management implementation. This system handles the transfer of keys between the base station and the subscriber station by using X.509 digital certificates and RSA public-key algorithm. Additional security is provided by refreshing the keys and connections at frequent intervals. If long keys (1024 bits) are used, the RSA algorithm is considered to be secure.

**Authentication**

User and device authentication for WiMAX consists of certificate support using Internet Engineering Task Force (IETF) Extensible Authentication Protocol. EAP is a structure designed to perform authentication through the use of functions that can negotiate with many different possible procedures. There are around 40 different procedures, called EAP methods, including some defined within the IETF standard and others that have been developed by outside entities. Some of the types of credentials that WiMAX can use for authentication purposes are digital certificates, smart cards and user name/password. In terminal devices, a X.509 digital certificate with both the MAC address and public key can perform device authentication as needed. Adding both user authentication and device authentication creates an additional layer of security.

**Wireless Control Messages**

Another authentication method used with WiMAX is support for control messages. This type of handshake is used to assure both the message authenticity and the integrity of the data that the message contains. CMAC (Cipher-based Message Authentication Code) uses a block cipher algorithm while HMAC (keyed-Hash Message Authentication Code) used a hash function to combine with the secret key. Both of these types of schemes are supported by WiMAX [4].

**Fast Handovers**

The process of transferring a connected device from one base station to another is call a handover or hand-off. There are three handover options specified by IEEE 802.16e-2005 but support is only required for one, the hard handover (HHO). This is a negotiation scheme that establishes identification and communication with a new base before releasing the connection with the old base. This method of handover can help to stop man-in-the-middle-attacks.

**Security Attacks**

Wi-Fi and WiMAX use different physical and data layers. As a result, security attacks can differ depending on which scheme is in place.

**Wi-Fi Security Attacks**

Being the older, more prevalent wireless standard, Wi-Fi has long been battered by security attacks from all sides. According to Ryan Paul in his April 25, 2007 article "Security researchers are beginning to note
increasing instances of so-called “evil twin” attacks, in which a malicious user sets up an open Wi-Fi network and monitors traffic in order to intercept private data [5].” Some of the other types of security threats that have been used on Wi-Fi networks are identity theft in the form of MAC spoofing, man-in-the-middle attacks, Denial-of-Service (DoS) attacks and network injection attacks where intruders inject commands into the network to re-configure it.

**WiMAX Security Attacks**

Jamming and packet scrambling are the general kinds of attacks that can most affect WiMAX’s physical layer. Signals in the lower frequencies that cross or are in close proximity to the WiMAX antenna can produce second and third harmonic waves that interfere and can overload the WiMAX signal. For example, take a 850 MHz signal, and you will find a second harmonic, although not as strong, at 1700 MHz (2 x 850). A third harmonic, much weaker, will be located at 2550 MHz (3 x 850). Because WiMAX is transmitted over frequency bands that are licensed, unintentional jamming is rare. Taking a spectrum analysis at intervals can mitigate constant jamming, whether malicious or not.

Within the Data Link Layer of the network stack, digital certificates work very well for establishing the identity of a mobile station to a base station. However, a simple one-way authentication could allow an opportunity for intruders to create a rogue base station and snoop traffic. Authentication using EAP-TLS will enable both the base station and the mobile station to use X.509 certificates to establish their legitimacy [6].

**Conclusion**

Most widespread and widely used inventions go through a series of changes as they go from novelty to commonplace. Do you recall how the bicycle went from a large wheel in front and a small wheel in back to its present day evenly sized wheels? Wi-Fi has seen much improvement in the years since its creation. Currently, using the latest security algorithms and being aware of device setup issues, Wi-Fi is considered safe for transferring data and communications. WiMAX is every bit as safe, if not more so because it was designed with security levels in mind from the beginning. With layer upon layer of authentication, authorization and encryption in place, WiMAX is ready right out of the box to perform safely. With careful attention to setup details and with moderate maintenance practices, devices, which utilize either of these standards, can be used in security-sensitive applications.

**References**


About the Author

Judy M. Hartley is a Software Application Engineer in the Software and Solutions Group. She earned her B.S. in Computer Engineering at Virginia Tech in 2001. Right after graduation, she began working for Intel, moving almost 3000 miles to Chandler, Arizona. As a Product Development Engineer she worked on testing and production readiness of set-top box chips. Because she missed the rain, in 2005 she relocated to one of Intel’s northwest locations and turned her attention to software and software enabling.

§